AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: s/Tiffany Edgmon 04/22/2024

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
Red iPhone cellular phone with IMEI
number 351138108948004

Case No: M-24-365-STE

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is attached and incorporated by reference.

FILED
APR 22 2024
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIS. OKLA.
BY _____, DEPUTY

Located in the Western District of Oklahoma, there is now:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2242(b)	Attempted Enticement of a Minor
18 U.S.C. § 2243(b)	Interstate Travel with Intent to Engage in a Sexual Act with a Minor
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Andrea Salazar, Homeland Security Investigations, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Andrea Salazar
Applicant's signature

Andrea Salazar
Special Agent
Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: April 22, 2024

Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Andrea Salazar, being first duly sworn, state as follows:

INTRODUCTION

1. I am currently employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so since July 2022. Prior, I was a federal police officer with Pentagon Force Protection Agency and had been so employed since August 2019. I hold a bachelor's degree in criminology and a Master of Public Administration from St. Mary's University. I also hold a Master of Science in Criminal Justice from Sam Houston State University.

2. I am currently assigned to HSI Office of the Resident Agent in Charge Oklahoma City, Oklahoma. As part of my various duties and responsibilities, I investigate federal criminal cybercrime violations. As it relates to cybercrime, I have gained experience conducting child exploitation and child pornography investigations. My working experience has been augmented by training I received at the Federal Law Enforcement Training Center. Moreover, I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators. I have become aware of numerous examples of child pornography. Additionally, I have had the opportunity to observe and review hundreds of images and videos of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2422(b) and 2423(b).

3. I am investigating the online activities of Bryan Devin CRUZ. As explained herein, there is probable cause to believe CRUZ committed the following crimes: Attempted Coercion and Enticement of a Minor, in violation of 18 U.S.C. § 2422(b); Interstate Travel with Intent to Engage in a Sexual Act with a Minor, in violation of 18 U.S.C. § 2423(b); and Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

4. This Affidavit seeks authorization to search CRUZ's red Apple iPhone cellular phone, with IMEI number 351138108948004 (the "**SUBJECT DEVICE**"), as further described in Attachment A, and seize the items described in Attachment B, which constitute instrumentalities, fruits, and evidence of the aforementioned crimes.

5. This Application would authorize the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying electronically stored data, particularly that described in Attachment B.

6. The **SUBJECT DEVICE** is currently secured at the HSI RAC Oklahoma City office, evidence control room, located at 3625 NW 56th St. Suite 300, Oklahoma City, Oklahoma 73112, in the Western District of Oklahoma. As set forth herein, there is probable cause to believe that CRUZ possessed, owned, and used the **SUBJECT DEVICE** to commit the aforementioned crimes.

7. The facts set forth in this Affidavit are based upon my personal observations and training, prior investigations and, where noted, information related to me by other law enforcement officers. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning

this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

8. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

9. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities. These photos are sometimes stored in cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

10. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications, as well as applications like Instagram. Additionally, individuals utilize their cellular devices to take and store pictures and keep notes. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer

conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual.

11. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during, and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information.

12. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the aforementioned crimes, but also forensic evidence that establishes how the **SUBJECT DEVICE** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT DEVICE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

13. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICE** consistent with the warrant. The examination may require authorities to employ techniques (including but not limited to computer-assisted scans of the entire medium) that might expose many parts of the **SUBJECT DEVICE** to human inspection in order to determine whether it is evidence described by the warrant.

14. *Manner of execution*. Because this warrant seeks only permission to examine

the **SUBJECT DEVICE** already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause to authorize execution of the warrant at any time in the day or night.

15. *Methods of examination*. In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the **SUBJECT DEVICE**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. "Computer" refers to any electronic, magnetic, optical, electrochemical, or other high-speed data processing device capable of performing logical or storage functions and includes any data storage facility or communications facility directly related to such a device. As used herein, "computer" also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. *See* 18 U.S.C. § 1030(e)(1).

b. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated

"GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers

control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I believe that the **SUBJECT DEVICE** has capabilities that allow it to serve as a wireless telephone, computer, digital camera, portable media player, GPS navigation device, and tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

BACKGROUND ON DISCORD

18. Discord is a voice, video, media, and text (chat) communication service/platform in which users can communicate in private chats, ranging from 1–10 users, or as part of a larger group/community called servers. Servers are also broken down into subcategories, or channels. Discord maintains these media, and text (chat) communications, whether they occurred on a server or in private chats. Discord asks each of their subscribers to provide certain identifying information when registering for an account. This information can include, but is not limited to: a username, subscriber's full name, date of birth, physical address, telephone numbers, other identifiers, and/or e-mail

addresses (which Discord can indicate if this email address has been verified or not). Information provided to and maintained by Discord by paying subscribers can include a means and source of payment (creditor bank account number).

a. Discord assigns a unique 18-digit User ID after an account is created. Discord and other providers of similar services, retain certain transactional information about the creation and use of each account on their systems. This information can include, but is not limited to: the date and time at which the account was created, the length of service, records of log-in (i.e., session) times and durations, friends list, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account.

b. Discord also has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. In some cases, account users will communicate directly with a provider, in this case, Discord, about issues relating to their account, such as technical problems, billing inquiries, and/or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user because of the communications.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS AND/OR ATTEMPT TO VIEW CHILD PORNOGRAPHY

19. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess and/or attempt to view child pornography:

a) Such individuals often receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b) Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c) Such individuals may possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines,

negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d) Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e) Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f) Such individuals also may correspond with and/or meet others to share information and materials, rarely completely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses,

telephone numbers, and usernames of individuals with whom they have been in contact and who share the same interests in child pornography.

g) Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if **CRUZ** or other co-conspirators use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the **SUBJECT PREMISES**, or on his person as set forth in Attachment A.

STATEMENT OF PROBABLE CAUSE

20. On or about April 5, 2024, Sergeant Spencer Sloan of the Moore Police Department ("MPD") was dispatched to 2816 Yorkshire Drive in Moore, Oklahoma, in the Western District of Oklahoma. A Moore resident, T.L., was reporting someone peeking into her thirteen-year-old daughter's ("Jane Doe") window.

21. Upon his arrival, Sgt. Sloan deployed the department's drone that utilizes thermal imaging to survey the area for any possible suspects. Almost immediately, Sgt. Sloan located a heat signature in the backyard of 2813 Yorkshire Circle. Sgt. Sloan informed officers of his findings, and the subject began to move to the west. The subject continued westbound in the creek and hopped a fence into a backyard of a residence (2824 Kings Road). The subject then hopped into the backyard of 2820 Kings Road and then walked from the backyard to the front of the residence. The subject walked north until he was apprehended in front of 2824 Kings Rd. This was all recorded via the drone. MPD

Officer Koalton R. Keller asked the subject to identify himself. The subject lied about his name and date of birth. Ultimately, the subject was identified as CRUZ. A red iPhone was located underneath a vehicle near CRUZ's location at the time of his arrest.

22. Sgt. Sloan then made his way to T.L.'s residence and spoke to T.L. According to T.L., she confiscated Jane Doe's laptop. T.L. allowed Sgt. Sloan to view the laptop where he observed messages between Jane Doe ("T" on discord) and "Alex." The conversation contained a few days' worth of messages. Several messages were sexual in nature. Jane Doe sent a photo to "Alex" depicting her vaginal area with the vagina covered with a hand. Sgt. Sloan confirmed the picture was sent by Jane Doe due to the red lights in the background that Jane Doe had in her room. Some of the messages were from "Alex" stating he wanted to use Jane Doe "like a toy.

23. MPD Detective Ryan Minard spoke to T.L., who advised the laptop belonged to Jane Doe's father S.P. who lived at another residence. Contact was made with the father, who consented to a search of the laptop.

24. Detective Minard observed on the discord app, on the laptop, that CRUZ was going by "Alex <3" as his username and Jane Doe was going by "T" as her username. CRUZ and Jane Doe communicated back and forth for several days. CRUZ made statements to Jane Doe about videos and pictures and how he knows Jane Doe has sent pictures to other people online. Jane Doe sent CRUZ a photograph of her while nude from the waist down. Cruz asked Jane Doe to face the camera and spread her legs for him. CRUZ asked Jane Doe to call on discord and they had multiple conversations through discord.

25. Cruz and Temperance met online using an application called "Discord" to communicate. Bryan advised Temperance that he went to Southmoore and Temperance stated she was completing online school. During the conversation, Cruz asked Temperance how old she was, and she stated she was 13 years old about to turn 14. Cruz advised back that her age was okay in the conversation.

26. CRUZ told Jane Doe he wanted to "smash"[1] and asked how they could meet up. Jane Doe also expressed a desire to run away. Jane Doe talked about the cameras that were at her dads' house and how mother had less cameras. Jane Doe also advised her older brother turned the cameras around at her mom's house.

27. CRUZ told Jane Doe that they could meet up outside of her residence. CRUZ then talked about how he can't wait to be inside Jane Doe and for her body to take the shape of his. CRUZ then talked about making plans to sneak into Jane Doe's window when her mother goes to sleep.

28. On April 6, 2024, CRUZ traveled from Texas to Jane Doe's residence. CRUZ asked Jane Doe when to come to the house. The two talked back and forth waiting for T.L. to go to bed. CRUZ asked Jane Doe which window was her window so not to go to the wrong one. In the chat, Jane Doe told CRUZ to come back after running away from the window and that not to worry because Jane Doe's mother thought it was "Chris." At that point in the conversation, T.L. contacted police and the resulting response began.

---

[1] Based on my training and experience, "smash" is a slang term meaning to have sex.

29. CRUZ was interviewed by Detective Minard. After his interview, CRUZ asked Detective Minard if he would be allowed to make any phone calls. Detective Minard stated CRUZ would be allowed to make phone calls if he could remember their phone numbers, to which CRUZ stated he could not. Detective Minard asked CRUZ for consent to open CRUZ's red iPhone but not go through it to help CRUZ get phone numbers out of the phone. CRUZ agreed by stating, "yes." CRUZ also provided the passcode to the red iPhone, when asked.

30. On April 10, 2024, Detective Minard spoke to M.E., who identified herself as CRUZ's wife. She stated that they lived at 3524 Marwick Drive, Plano, Texas. She also informed Detective Minard that CRUZ had told her he was traveling to a friend's wedding in Texas.

31. Through the use of law enforcement databases, it was discovered that on September 10, 2020, Dropbox LLC self-reported user doe00084@gmail.com/ESP, User ID: 3196730080, for uploading 19 images/videos of child pornography. Three of the IP addresses associated with the CyberTip came back to Andrea Vilchis, CRUZ's girlfriend during that period of time. Six other IP addresses associated with the CyberTip were traced back to Jorge Alvarez, CRUZ's roommate during that period of time. The remaining two IP addresses were associated with Ruth Pina, CRUZ's mother. The resulting investigation did not lead to any criminal charges.

CONCLUSION

a. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property,

evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are on the **SUBJECT DEVICE** described in Attachment A. I respectfully request this Court issue a search warrant for the **SUBJECT DEVICE** described in Attachment A to seize the items described in Attachment B.

Andrea Salazar
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 22nd day of April, 2024.

SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant seeks to search CRUZ's red Apple iPhone cellular phone, with assigned IMEI number 351138108948004. The **SUBJECT DEVICE** is currently secured at the HSI Resident Agent in Charge Oklahoma City Office, evidence control room, located at 3625 NW 56th St. Suite 300, Oklahoma City, OK 73112, and it is depicted below:

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

All records on the **SUBJECT DEVICE** described in Attachment A that relate to violations of the aforementioned offenses:

I. Digital Evidence

1. Any passwords, password files, test keys, encryption codes, or other information necessary to access the **SUBJECT DEVICE;**

2. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device described in Attachment A, that show the actual user(s) of the computer or digital device during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the device; MAC IDs and/or Internet Protocol addresses used by the device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software; evidence of the absence of such malicious software, or of the presence or absence of security software designed to detect malicious software;

3. Evidence that the device was attached to or used as a data storage device for some other device, or that another device was attached to the device; and

4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device;

II. Records, Documents, and Visual Depictions

5. Any records, documents, or materials, including correspondence in support of the search warrant application in any form including Instagram, or any other social media platform;

6. Any records, documents, or materials, including any correspondence, that involve any communication with any person that appear to be coercive in nature for the purposes of grooming or obtaining images from any person;

7. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

8. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

9. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

10. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction

of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

11. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

12. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

13. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet on any app installed on the **SUBJECT DEVICE**;

14. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received;

15. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and/or notes associated with child pornography or those who collect, disseminate, or trade in child pornography; and

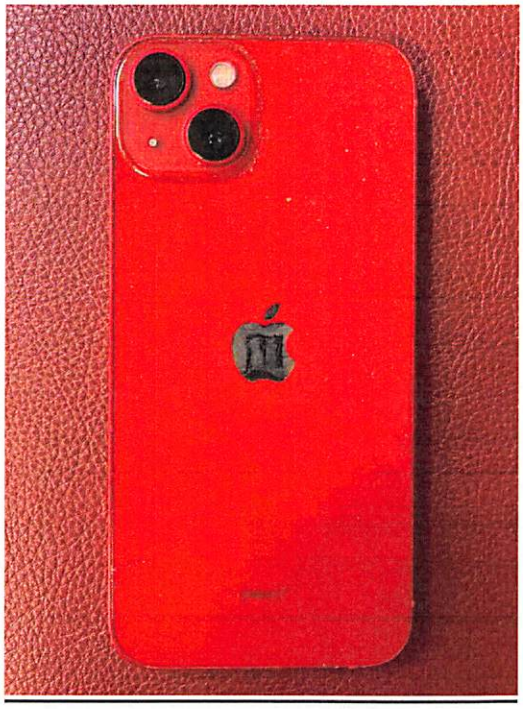
16. Any records, documents, materials, videos, or photographs that would allow investigators to ascertain who used the **SUBJECT DEVICE**.

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant seeks to search CRUZ's red Apple iPhone cellular phone, with assigned IMEI number 351138108948004. The **SUBJECT DEVICE** is currently secured at the HSI Resident Agent in Charge Oklahoma City Office, evidence control room, located at 3625 NW 56th St. Suite 300, Oklahoma City, OK 73112, and it is depicted below:



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

All records on the **SUBJECT DEVICE** described in Attachment A that relate to violations of the aforementioned offenses:

I. Digital Evidence

1. Any passwords, password files, test keys, encryption codes, or other information necessary to access the **SUBJECT DEVICE;**

2. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device described in Attachment A, that show the actual user(s) of the computer or digital device during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the device; MAC IDs and/or Internet Protocol addresses used by the device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software; evidence of the absence of such malicious software, or of the presence or absence of security software designed to detect malicious software;

3. Evidence that the device was attached to or used as a data storage device for some other device, or that another device was attached to the device; and

4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device;

II. Records, Documents, and Visual Depictions

5. Any records, documents, or materials, including correspondence in support of the search warrant application in any form including Instagram, or any other social media platform;

6. Any records, documents, or materials, including any correspondence, that involve any communication with any person that appear to be coercive in nature for the purposes of grooming or obtaining images from any person;

7. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

8. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

9. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

10. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction

of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

11. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

12. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

13. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet on any app installed on the **SUBJECT DEVICE**;

14. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received;

15. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and/or notes associated with child pornography or those who collect, disseminate, or trade in child pornography; and

16. Any records, documents, materials, videos, or photographs that would allow investigators to ascertain who used the **SUBJECT DEVICE**.

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.